IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF ILLINOIS

JANE DOE, by and through next friend **JOHN DOE**, **RICHARD ROBINSON**, and **YOLANDA BROWN**, on behalf of themselves and all other persons similarly situated, known and unknown, Plaintiffs, v. **APPLE INC.**, Defendant.	Case No. 3:22-cv-2575-RJD

APPLE INC.'S ANSWER AND AFFIRMATIVE DEFENSES TO PLAINTIFFS' AMENDED CLASS ACTION COMPLAINT

Apple Inc. ("Apple"), by its undersigned counsel, states the following answers and affirmative defenses. By omitting headings, footnotes, and images found in Plaintiffs' complaint, Apple does not admit—and specifically denies—the accuracy, completeness, and applicability of any factual content conveyed by such matters. Stating further, and for the avoidance of doubt, Apple construes all references to "biometric data" or "Biometric Data," herein and in Plaintiffs' Complaint, to mean only: (1) a "biometric identifier" or (2) "biometric information," as those two terms are defined in 740 ILCS 14/10.

1. Plaintiffs allege that Defendant violated BIPA by profiting from the biometric identifiers and biometric information (collectively, "Biometric Data") of Illinois citizens via Defendant's Photos software application ("Photos App"). For the reasons discussed in greater detail below, Defendant's violations of BIPA pose a serious threat of permanent harm to Illinois citizens.

ANSWER: Apple admits only that it produces a Photos app. The remaining allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies such allegations and further states that the Complaint fails to state a claim against Apple.

2. Defendant's Photos App comes pre-installed on Defendant's phones, tablets, and computers ("Apple Devices"). The Photos App, which cannot be removed or modified, automatically collects face Biometric Data from Apple Device users' photographs. Defendant's Photos App collects Biometric Data without the knowledge or informed written consent of the Apple Device users or Apple Device nonusers—including minors—who appear in photographs on Apple Devices. Users of Apple Devices are not told by Defendant that it is collecting face Biometric Data, and cannot disable Defendant's collection of face Biometric Data. Contrary to Defendant's public representations, moreover, Defendant collects and possesses Biometric Data on its servers.

ANSWER: Apple admits that the Photos app is available for Apple iPhones, iPads, and Macs. Apple denies the remaining allegations in this paragraph.

3. Defendant violates BIPA Section 15(c) by profiting from the Biometric Data it collects and possesses. Defendant profits from the face Biometric Data of Apple device users and nonusers because it uses the facial recognition capabilities of its Photos App, which violate BIPA, to market and sell its devices and software.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

4. Through this lawsuit, Plaintiffs, on behalf of a similarly situated class, seek to enjoin Defendant from profiting from their Biometric Data in violation of BIPA, and seek to obtain actual and statutory damages for their injuries.

ANSWER: Apple admits only that this paragraph purports to summarize Plaintiffs' claims. Apple denies all substantive allegations in this paragraph, denies that this action may be maintained individually or on behalf of any class, and further states that the Complaint fails to plead any cause of action against Apple.

5. Plaintiffs allege that Defendant violated BIPA by profiting from their biometric identifiers and biometric information.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

6. Plaintiffs seek to represent a class of individuals whose face geometries were collected, stored, and/or used by Defendant, including through the use of Defendant's Photos App.

ANSWER: Apple admits only that this paragraph purports to summarize Plaintiffs' claims. Apple denies all substantive allegations in this paragraph, denies that this action may be maintained individually or on behalf of any class, and further states that the Complaint fails to plead any cause of action against Apple.

7. Plaintiffs have suffered significant damage, as more fully described herein, because Defendant has collected their Biometric Data without their knowledge, consent, or understanding, thereby materially decreasing the security of this intrinsically inalterable information, and substantially increasing the likelihood that Plaintiffs will suffer as victims of fraud and/or identity theft.

ANSWER: Denied.

8. Plaintiffs seek actual damages in addition to statutory damages, as provided below in the Prayer for Relief.

ANSWER: Apple admits only that this paragraph purports to summarize Plaintiffs' claims. Apple denies all substantive allegations in this paragraph, denies any allegations of wrongdoing, and further states that the Complaint fails to plead any cause of action against Apple.

9. The remedies Plaintiffs seek are remedial, and not penal, in nature.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

10. Plaintiff Jane Doe, a minor, is a resident of O'Fallon in St. Clair County, Illinois. John Doe, Jane Doe's next friend, is also a resident of O'Fallon in St. Clair County, Illinois.

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

11. Plaintiff Richard Robinson is a resident of Troy in Madison County, Illinois.

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

12. Plaintiff Yolanda Brown is a resident of Godfrey in Madison County, Illinois.

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

13. Plaintiffs' face geometries have been scanned by Defendant, and their Biometric Data were collected, stored, and used by Defendant, as more fully described herein.

ANSWER: Denied.

14. Defendant is a California corporation that is registered to and does conduct business throughout Illinois.

ANSWER: Apple admits that it is a California corporation that is registered to and does conduct business in Illinois. Apple denies any remaining allegations in this paragraph.

15. Defendant is a "private entity" under the meaning of BIPA. 740 ILCS 14/10.

ANSWER: Apple admits that it is a corporation, which is included within BIPA's definition of "private entity," but denies that the Complaint alleges activity to which BIPA applies or that Apple has violated any obligation under BIPA.

16. This Court has personal jurisdiction over Defendant because, during the relevant time period, Defendant was registered to do business in Illinois, conducted business in Illinois, committed the violations alleged in Illinois, and purposefully availed itself of the laws of Illinois for the specific transactions and occurrences at issue.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required.

17. St. Clair County is an appropriate venue for this litigation because Defendant does business in St. Clair County, and is therefore a resident of St. Clair County. 735 ILCS 5/2-102.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

18. In addition, the transactions and occurrences out of which the causes of action pleaded herein arose or occurred, in part, in St. Clair County.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

19. "Biometrics" refers to "biology-based set[s] of measurements." Rivera v. Google Inc., 238 F. Supp. 3d 1088, 1094 (N.D. Ill. 2017). Specifically, "biometrics" are "a set of measurements of a specified physical component (eye, finger, voice, hand, face)." Id. at 1296.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple admits that this paragraph quotes or paraphrases selected portions of the *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088 (N.D. Ill. 2017) opinion, reserves all arguments with regard to the *Rivera* opinion, and refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

20. BIPA was enacted in 2008 in order to safeguard Biometric Data due to the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Sess. No. 276. BIPA is codified as Act 14 in Chapter 740 of the Illinois Compiled Statutes.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

21. As set forth in BIPA, biologically unique identifiers, such as scans of individuals' facial geometry, cannot be changed. 740 ILCS 14/5(c). As is likewise explained in BIPA, the inalterable nature of individuals' biologically unique identifiers presents a materially heightened risk of serious harm when Biometric Data is not protected in a secure and transparent fashion. 740 ILCS 14/5(d)–(g).

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

22. As a result of the need for enhanced protection of Biometric Data, BIPA imposes various requirements on private entities that collect or possess individuals' biometric identifiers, including scans of individuals' facial geometries.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

23. Among other things, BIPA regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g).

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

24. BIPA applies to entities that interact with two forms of Biometric Data: biometric "identifiers" and biometric "information." 740 ILCS 14/15(a)–(e).

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

25. "Biometric identifiers" are physiological, as opposed to behavioral, characteristics. Examples include, but are not limited to, face geometry, fingerprints, voiceprints, DNA, palmprints, hand geometry, iris patterns, and retina patterns. As the Illinois General Assembly has explained: Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions. 740 ILCS 14/5(c). Moreover, a person cannot obtain new DNA or new fingerprints or new eyeballs for iris recognition, at least not easily or not at this time. Replacing a biometric identifier is not like replacing a lost key or a misplaced identification card or a stolen access code. The Act's goal is to prevent irretrievable harm from happening and to put in place a process and rules to reassure an otherwise skittish public. Sekura v. Krishna Schaumburg Tan, Inc., 2018 IL App (1st) 180175, ¶ 59, 115 N.E.3d 1080, 1093, appeal denied, 119 N.E.3d 1034 (Ill. 2019).

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple admits that this paragraph quotes or paraphrases selected portions of the *Sekura v Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175, 115 N.E.3d 1080, *appeal denied*, 119 N.E.3d 1034 (Ill. 2019) opinion, reserves all arguments with regard to the *Sekura* opinion, and refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

26. In BIPA's text, the General Assembly provided a non-exclusive list of protected "biometric identifiers," including "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. In this case, the biometric identifiers at issue are the scans of face geometries of individuals, including Plaintiffs, collected by Defendant via its proprietary software without any notice to or consent from the individuals whose biometric identifiers are collected.

ANSWER: Apple denies the allegations of the final sentence in this paragraph. The remaining allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

27. "Biometric information" consists of biometric identifiers used to identify a specific person. BIPA defines "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." Id. (emphasis added).

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

28. In BIPA, the General Assembly identified four distinct activities that may subject private entities to liability: (1) collecting Biometric Data, 740 ILCS 14/15(b); (2) possessing Biometric Data, 740 ILCS 14/15(a); (3) profiting from Biometric Data, 740 ILCS 14/15(c); and (4) disclosing Biometric Data, 740 ILCS 14/15(d). BIPA also created a heightened standard of care for the protection of Biometric Data. 740 ILCS 14/15(e).

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

29. As the Illinois Supreme Court has held, BIPA "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." Rosenbach v. Six Flags Entm't Corp., 2019 IL 123186, ¶ 33, 129 N.E.3d 1197, 1206 (Ill. 2019). The Illinois Supreme Court further held that when a private entity fails to comply with BIPA "that violation constitutes an invasion, impairment, or denial of the statutory rights of any person or customer whose biometric identifier or biometric information is subject to the breach." Id.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple admits that this paragraph quotes or paraphrases selected portions of the *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, 129 N.E.3d 1197, 1206 (Ill. 2019) opinion, reserves all arguments with regard to the *Rosenbach* opinion, and refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

30. BIPA establishes categories of prohibited conduct related to Biometric Data, and establishes requirements that parties must follow when interacting with Biometric Data. As Section 15(b) provides: No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first: (1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative. 740 ILCS 14/15(b).

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

31. To "collect" means "to bring together into one body or place," or "to gather or exact from a number of persons or sources."

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

32. Collection, therefore, is the act of gathering together, and is separate from possession, which is not an element of collection.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

33. BIPA imposes three requirements that must be satisfied before any private entity may "collect" biometric information: (a) First, the private entity must inform the individual in

writing that the individual's biometric information is being collected or stored. 740 ILCS 14/15(b)(1). (b) Second, the private entity must inform the individual in writing of the purpose and length of time for which their biometric information is being collected, stored, and used. 740 ILCS 14/15(b)(2). (c) Finally, the private entity must receive a written release executed by the individual. 740 ILCS 14/15(b)(3).

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

34. BIPA defines a "written release," outside the employment context, to mean "informed written consent." 740 ILCS 14/10.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

35. With respect to possession of Biometric Data, BIPA provides as follows: A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. 740 ILCS 14/15(a). Entities in possession of Biometric Data therefore must develop and make public a written policy containing a retention schedule for Biometric Data, as well as guidelines for the destruction of Biometric Data. Id.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

36. BIPA requires that the required public, written policy include information about how the entity will destroy Biometric Data. Id.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

37. The plain and ordinary meaning of the word "possession" is "the act of having or taking into control" or "control or occupancy of property without regard to ownership."

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

38. A private entity that controls Biometric Data, therefore, possesses Biometric Data under Section 15(a).

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

39. Section 15(a) regulates Biometric Data that is controlled by a private entity regardless of whether that entity owns the Biometric Data.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to

paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

40. Here, for example, Defendant controls Plaintiffs' Biometric Data, even though Defendant does not own that data. Therefore, as alleged in further detail below, Defendant possesses Plaintiffs' Biometric Data under Section 15(a).

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

41. BIPA additionally bars private entities from profiting from Biometric Data. Section 15(c) provides as follows: No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information. 740 ILCS 14/15(c).

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

42. Section 15(c) is an unqualified prohibition on profiting from Biometric Data. Section 15(c) applies to this case, for among other reasons, because Defendant developed the face recognition "feature" of its Photos App in order to competitively position its devices and software in the marketplace, compete with other software applications, and thereby profit.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies any allegation that it violated Section 15(c) of BIPA, refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith.

43. Extracting an individual's face geometry data in order to confirm a subsequent match of the individual's face—also known as "facial recognition" or "faceprinting"—uses biological characteristics to verify an individual's identity.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

44. Use of facial recognition technology can be highly lucrative. The global facial recognition market size is expected to grow dramatically—according to one source, from $3.2 billion in 2019 to $7 billion by 2024.

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

45. However, the potential dangers of the use of facial recognition technology and other biometric identifiers are widely known.

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

46. "Stolen biometric identifiers . . . can be used to impersonate consumers, gaining access to personal information."

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth any biometric identifier or theft or use of any biometric identifier. Apple lacks knowledge or information sufficient to form a belief as to others' uses of biometric identifiers and therefore denies any remaining allegations in this paragraph.

47. Unlike other identifiers such as Social Security or credit card numbers, which can be changed if compromised or stolen, biometric identifiers linked to a specific voice or face cannot be modified—ever. These unique and permanent biometric identifiers, once exposed, leave victims with no means to prevent identity theft and unauthorized tracking. Recognizing this, the Federal Trade Commission has urged companies using facial recognition technology to ask for consent before scanning and extracting Biometric Data from photographs.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth with respect to Plaintiffs or Apple any biometric identifiers or biometric data or theft, use, exposure, scanning, or extracting of any biometric identifiers or biometric data. Apple lacks knowledge or information sufficient to form a belief as to others' use, scanning, or extraction of biometric identifiers or biometric data and therefore denies any remaining allegations in this paragraph.

48. The threats posed by facial recognition technology can be more insidious than the threats posed by the use of other biometric information, such as fingerprints. Indeed, as commentators have recognized, "facial recognition creates acute privacy concerns that fingerprints do not." Once a person or entity has an individual's facial Biometric Data: [T]hey can get your name, they can find your social networking account, and they can find and track you in the street, in the stores that you visit, the . . . buildings you enter, and the photos your friends post online. Your face is a conduit to an incredible amount of information about you, and facial recognition technology can allow others to access all of that information from a distance, without your knowledge, and in about as much time as it takes to snap a photo.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth with respect to Plaintiffs or Apple any facial biometric data or use or possession of any facial biometric data. Apple lacks knowledge or information sufficient to form a belief as to others' use or possession of facial biometric data or facial recognition technology and therefore denies any remaining allegations in this paragraph.

49. Researchers have even demonstrated the ability to "infer personally predictable sensitive information through face recognition."

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph, and therefore denies the same.

50. Further, facial recognition technology may "be abused in ways that could threaten basic aspects of our privacy and civil liberties[:]"Biometrics in general are immutable, readily accessible, individuating, and can be highly prejudicial. And facial recognition takes the risks inherent in other biometrics to a new level. Americans cannot take precautions to prevent the collection of their image. We walk around in public. Our image is always exposed to the public. Facial recognition allows for covert, remote, and mass capture and identification of images, and the photos that may end up in a data base include not just a person's face but also what she is wearing, what she might be carrying, and who she is associated with. This creates threats to free expression and to freedom of association that are not evident in other biometrics.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth with respect to Plaintiffs or Apple any biometric data or use, abuse, capture, prejudice, or threat relating to biometric data. Apple lacks knowledge or information sufficient to form a belief as to others' use, abuse, capture, or identification of images or biometric data and therefore denies any remaining allegations in this paragraph.

51. Many experts believe that "facial recognition technology is the most uniquely dangerous surveillance mechanism ever invented."

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph, and therefore denies the same.

52. Because of these dangers, "privacy protections," such as those found in BIPA, are necessary for "all facial recognition technologies, including those that do not individually identify consumers."

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph, and therefore denies the same. Stating

further, privacy is one of Apple's core values; Apple therefore designs its products and features from the ground up with privacy in mind so they protect users' privacy and give users control over their information.

53. Indeed, the Illinois Supreme Court has held that in BIPA the Illinois "General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." Rosenbach, 129 N.E.3d at 1206.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple admits that this paragraph quotes or paraphrases selected portions of the *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, 129 N.E.3d 1197, 1206 (Ill. 2019) opinion, reserves all arguments with regard to the *Rosenbach* opinion, and refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

54. In so holding, the Court explicitly recognized the "difficulty in providing meaningful recourse once a person's biometric identifiers or biometric information has been compromised." Id. As it further held, "[t]he situation is particularly concerning, in the legislature's judgment, because [t]he full ramifications of biometric technology are not fully known.'" Id. (citing BIPA).

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple admits that this paragraph quotes or paraphrases selected portions of the *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186, 129 N.E.3d 1197, 1206 (Ill. 2019) opinion, reserves all arguments with regard to the *Rosenbach* opinion, and refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

55. Defendant acknowledges that "face data is . . . so personal" it warrants "extraordinary measures to protect it."

ANSWER: Apple admits that this paragraph quotes or paraphrases portions of a page on the Apple website (https://www.apple.com/privacy/control/), refers to the text of the page in its entirety, and denies any attempt to paraphrase or characterize the page's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

56. With respect to face data used to unlock Apple Devices, Defendant claims that it takes "extraordinary measures," including encrypting it, storing it on a "secure enclave," preventing access to the data by the operating system or any applications, and ensuring that it is "never stored on Apple servers or backed up to iCloud or anywhere else."

ANSWER: Apple admits that this paragraph quotes or paraphrases portions of a page on the Apple website (https://www.apple.com/privacy/control/), refers to the text of the page in its entirety, and denies any attempt to paraphrase or characterize the page's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

57. Defendant also represents to the public that in order to "protect[] your privacy," in the Photos app, "all the face recognition and scene and object detection are done completely on your device."

ANSWER: Apple admits that this paragraph purports to quote or paraphrase portions of a support article on the Apple website (https://support.apple.com/en-us/HT207368), refers to the text of the article in its entirety, and denies any attempt to paraphrase or characterize the article's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph or its footnote.

58. Storing Biometric Data on personal devices (as opposed to on a server) does not remove the substantial dangers associated with Biometric Data, because personal devices are intrinsically vulnerable to hackers and other malicious bad actors. Instead, storing Biometric Data on personal devices creates an independent threat of serious harm that is associated with each personal device that contains Biometric Data.

ANSWER: Denied.

59. Moreover, Biometric Data may persist on discarded devices. "Realistically, unless you physically destroy a device, forensic experts can potentially extract data from it." The Federal Trade Commission has recognized that sensitive data on individual devices poses grave risks, including of identity theft.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth with respect to Plaintiffs or Apple any biometric data or extraction of biometric data. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

60. The use of Biometric Data "leads to the fear that a data breach or sale by one holder of a piece of a person's biometric information would compromise the security of all relationships that are verified by that same piece."

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth with respect to Plaintiffs or Apple any biometric data, data breach, or sale of biometric data. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

61. This fear is not based on mere conjecture. Biometric Data has been illicitly targeted by hackers. For example, a security firm recently uncovered a "major breach" of a biometric system used by banks, police, defense firms, and other entities. This breach involved exposure of extensive biometric and other personal data, including facial recognition data and fingerprints. Id.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth with respect to

Plaintiffs or Apple any biometric data or targeting or breach of biometric data. Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

62. Even anonymized Biometric Data poses risks. For example, according to a recent report: In August 2016, the Australian government released an "anonymized" data set comprising the medical billing records, including every prescription and surgery, of 2.9 million people. Names and other identifying features were removed from the records in an effort to protect individuals' privacy, but a research team from the University of Melbourne soon discovered that it was simple to re-identify people, and learn about their entire medical history without their consent, by comparing the dataset to other publicly available information, such as reports of celebrities having babies or athletes having surgeries. Indeed, "[t]here is a growing skepticism in the field of data protection and privacy law that biometric data can never truly be deidentified or anonymized."

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth with respect to Plaintiffs or Apple any biometric data, re-identification of anonymous data, or release of biometric data. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

63. The collection and use of Biometric Data is especially problematic in relation to the collection of Biometric Data from minors, who cannot provide informed consent and may be unaware of the serious harms that can result from the release of Biometric Data.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth the collection or use of minors' biometric data. Apple lacks knowledge or information sufficient to form a belief as to the truth of the incomplete hypothetical following the comma, and therefore denies the same.

64. The heightened sensitivity of minors' personal data has been recognized by the federal government in the Children's Online Privacy Protection Act, which provides special protections for children's personal data.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint implicate the Children's Online Privacy Protection Act ("COPPA"), refers to COPPA for its complete text, and denies any attempt to paraphrase or characterize COPPA and all allegations inconsistent therewith.

65. "The monetization of children's biometric . . . data is also concerning even if such data are anonymized." Even "before minors come of age their immutable biometric or health-related data could be collected[.]" Once a minor's biometric information is compromised, the damage can be permanent.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth with respect to Plaintiffs or Apple any biometric data or collection or compromise of biometric data. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

66. Defendant's devices have been repeatedly and seriously breached. For example, in 2015, hackers snuck malware onto thousands of apps on the iPhone App Store, impacting hundreds of millions of people, and hijacking their Apple Devices to steal potentially sensitive user information.

ANSWER: The allegations in this paragraph are immaterial and impertinent and, accordingly, should be stricken. Fed. R. Civ. P. 12(f). To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

67. Defendant includes facial recognition technology as a "feature" of its Photos App that is included by default in its operating systems as well as pre-installed on its devices sold to customers ("Photo Sorting Software").

ANSWER: The allegations in this paragraph are vague and ambiguous by virtue of their use of the undefined phrases "facial recognition technology," "operating systems," and "devices sold to customers." Apple admits only that the Photos app is built into certain operating systems for certain devices designed by Apple. Apple denies any remaining allegations in this paragraph.

68. The Photo Sorting Software uses biometric identifiers collected from images to create individualized groupings of all photographs that include a particular person, such as a friend or family member of the user.

ANSWER: Denied.

69. Defendant began automatically collecting the Biometric Data at issue through iPhones, iPads, and iPod Touch devices via its Photos App with the release of its operating system iOS, version 10, which was released to public beta testers on July 7, 2016 and to the general public on September 13, 2016. Defendant likewise began automatically collecting Biometric Data through Macintosh computers via its public-beta release of macOS Sierra on July 7, 2016 and to the general public on September 20, 2016. These operating systems included the Photos App with facial recognition.

ANSWER: The allegations in this paragraph are vague and ambiguous by virtue of their use of the undefined phrases "released to public beta testers" and "facial recognition." Apple admits only that the Photos app was built into iOS 10, which Apple released as a free update on September 13, 2016, and macOS Sierra, which Apple released as a free update on September 20, 2016. Apple denies the remaining allegations in this paragraph.

70. Defendant includes its Photos App on iOS, iPadOS, and MacOS operating systems, and on Apple Devices. Defendant sells Apple Devices with those operating systems and the Photos App preinstalled.

ANSWER: Apple admits that the Photos app is built into iOS, iPadOS, and MacOS and that Apple sells certain devices running these operating systems. Apple denies any remaining allegations in this paragraph.

71. The facial recognition "feature" of Defendant's Photos App functions by scanning a user's photo library for faces, and then, using facial recognition technology that extracts biometric identifiers from photographs, grouping photographs of faces, including in the user's People albums.

ANSWER: The allegations in this paragraph are vague and ambiguous by virtue of their use of the undefined phrases "facial recognition" and "facial recognition technology." Apple admits that the Photos app attempts to detect the faces in photos on the user's device and, if the Photos app detects a face, may sort a photo into a People album. Apple denies the remaining allegations in this paragraph or its footnote.

72. In U.S. Patent No. 9,977,952 (filed Oct. 31, 2016), Defendant explained this process as follows: Facial recognition (or recognition) relates to identifying a person represented in an image. Recognition can be accomplished by comparing selected facial features from a graphical face to a facial database. Facial recognition algorithms can identify faces by extracting landmarks corresponding to facial features from the image. For example, an algorithm may analyze the relative position, size, and shape of the eyes, nose, cheekbones, and jaw. Id. at 1:32–40.

ANSWER: Apple admits that it holds U.S. Patent 9,977,952. Apple refers to the text of the patent in its entirety and denies any attempt to paraphrase or characterize the patent's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

73. Accordingly, the Photos App creates a scan of face geometry, which BIPA defines as a "biometric identifier." See 740 ILCS 14/10.

ANSWER: Denied.

74. [redacted] The Photo Sorting Software, accordingly, collects biometric identifiers.

ANSWER: Denied.

75. Through its Photo Sorting Software, Defendant uses scans of face geometry to identify individuals, thereby collecting and possessing biometric information locally on Apple Devices as well as collecting and possessing biometric information on Defendant's servers.

ANSWER: Denied.

76. Defendant runs facial recognition algorithms on Apple Devices.

ANSWER: Denied.

77. Defendant stores Biometric Data taken from Apple Device users' image libraries in what Defendant calls a facial recognition database, or facial database, in the solid-state memory on users' Apple Devices.

ANSWER: Denied. Stating further, Apple states that all review and grouping of photos by the Photos app occurs entirely on the user's device, but that the Photos app does not create or rely on biometric data.

78. Not only does Defendant use face geometries to identify individuals, with iOS version 11, it uses face geometries to model users faces and track the users' expressions in real time. Defendant calls this "intelligent face recognition."

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph. Stating further, Apple refers to

https://developer.apple.com/documentation/arkit/tracking_and_visualizing_faces,

https://developer.apple.com/videos/play/tech-talks/601,

https://developer.apple.com/documentation/vision/tracking_the_user_s_face_in_real_time, and

https://www.apple.com/ios/photos

for their complete text and denies any attempt to paraphrase or characterize their complete text and all allegations inconsistent therewith.

79. Defendant has published the following visualization of the face geometry it creates from pictures in users' photo libraries:

ANSWER: Denied.

80. After creating facial templates, Defendant uses facial recognition algorithms to analyze digital photographs stored on its devices and automatically group photographs into

albums based on whether a person's face is in the photograph. Children and minors are included among those whose facial geometries are analyzed and grouped by Defendant.

ANSWER: Denied.

81. Defendant's facial recognition algorithms calculate a unique digital representation of faces based on geometric attributes, such as distance between the eyes, width of the nose, and other features.

ANSWER: Denied.

82. Defendant's software collects Biometric Data to group all photographs that include a particular person's face into an album or folder.

ANSWER: Denied.

83. Defendant creates a unique faceprint for every person appearing in any photograph stored using its Photos App.

ANSWER: Denied.

84. Defendant collects this face Biometric Data without obtaining consent, let alone the "informed written consent" required by BIPA.

ANSWER: Denied.

85. Defendant's devices, further, collect Biometric Data from all individuals, including minors, whose faces appear in Apple Device users' photographs—not just from Apple Device users.

ANSWER: Denied.

86. Defendant confirms these capabilities and seeks to profit from its collection of Biometric Data by advertising its Photos App as being able to "recognize the people, scenes, and objects in [photographs]."

ANSWER: Apple denies the allegations in this paragraph. Stating further, Apple refers to the version of the support article appearing at https://support.apple.com/en-us/HT207103 as of December 16, 2021, for its complete text and denies any attempt to paraphrase or characterize its complete text and all allegations inconsistent therewith.

*87. Defendant further advertises that its Photos App "uses advanced computer vision to scan all of your photos to s]ort [*sic*] your images by your favorite subjects — the people in your life."*

ANSWER: Apple admits that this paragraph purports to quote or paraphrase portions of a support article appearing at https://support.apple.com/en-us/HT207103, refers to the text of the article in its entirety, and denies any attempt to misstate, paraphrase, or characterize the article's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

88. In order to sort photos, Defendant admits that its Photos App uses "[i]ntelligent face and location identification."

ANSWER: Apple admits that this paragraph quotes or paraphrases portions of a page on the Apple website (https://www.apple.com/ios/photos/), refers to the text of that page in its entirety, and denies any attempt to paraphrase or characterize the page's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

89. Defendant advertises to users the ability "to find the exact photos you're looking for, based on who you were with or where you were when you took them."

ANSWER: Apple admits that this paragraph quotes or paraphrases portions of a page on the Apple website (https://www.apple.com/ios/photos/), refers to the text of that page in its entirety, and denies any attempt to paraphrase or characterize the page's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

90. Defendant collects biometric identifiers and biometric information for individuals whose faces appear in photographs stored on Apple Devices. These Biometric Data are catalogued on the Photos App.

ANSWER: Denied.

91. Defendant's collection of biometric identifiers and biometric information through its Photos App is automatic and occurs without the involvement or consent of an Apple Device user whenever a new photograph is stored on an Apple Device.

ANSWER: Denied.

92. Apple Device users cannot disable Defendant's facial recognition technology, and cannot prevent Defendant's collection of Biometric Data from occurring.

ANSWER: Denied.

93. Defendant provides no mechanism by which users or nonusers may opt out of the collection of their Biometric Data.

ANSWER: Denied.

94. Consumers who buy Apple Devices own the hardware but merely license the software necessary for the device to function. That software is wholly owned and controlled by Defendant.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple admits only that: (1) device users own and possess the device hardware and control their use of the devices and the software on the devices; and (2) the software license agreements cited in the footnote to this paragraph (https://www.apple.com/legal/sla/docs/iOS13_iPadOS13.pdf and https://www.apple.com/legal/sla/docs/macOSCatalina.pdf) state that the Apple Software (as defined in each agreement) "are licensed, not sold, to you by Apple Inc. ('Apple') for use only under the terms of this License. Apple [and/or Apple's] licensors retain ownership of the Apple Software itself and reserve all rights not expressly granted to you." Apple denies any remaining allegations in this paragraph.

95. Defendant's applicable End User License Agreements ("EULAs") provide as follows: "The software . . . [is] licensed, not sold, to you by Apple Inc. ('Apple') for use only under the terms of this License. Apple and its licensors retain ownership of the Apple Software itself and reserve all rights not expressly granted to you."

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the "applicable End User License Agreements ('EULAs')." Apple admits only that this paragraph cites and quotes or paraphrases portions of the iOS and iPadOS Software License Agreement for iOS 13 and iPadOS13 (https://www.apple.com/legal/sla/docs/iOS13_iPadOS13.pdf, the "iOS 13 and iPadOS 13 SLA"), refers to the text of the iOS 13 and iPadOS 13 SLA in its entirety, and denies any attempt to paraphrase or characterize the license's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

96. The Apple Device user is granted "a limited non-exclusive license to use the Apple Software on a single Apple-branded Device" and cannot alter the software.

ANSWER: Apple admits only that this paragraph cites and quotes or paraphrases portions of the iOS 13 and iPadOS 13 SLA, refers to the text of the iOS 13 and iPadOS 13 SLA in its entirety, and denies any attempt to paraphrase or characterize the license's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

97. Because disabling facial recognition is not permitted by Defendant, the use of Apple Devices to take or store photographs is conditioned on the collection of Biometric Data.

ANSWER: Denied.

98. Defendant indiscriminately collects Biometric Data for all photographic subjects, including customers, non-customers, and minors incapable of providing informed consent.

ANSWER: Denied.

99. Defendant publishes the "Machine Learning Journal," which contains posts dedicated to describing the development of various of Defendant's products. In one such post from November 2017, Defendant described the use of deep learning to facilitate the facial recognition feature used by the Photos App as packaged in iOS version 10. Defendant describes the below figure as a "[f]ace detection workflow."

ANSWER: Apple admits that it publishes the Machine Learning Journal (https://machinelearning.apple.com/). Apple further admits that this paragraph purports to quote from or paraphrase portions of the November 2017 article "An On-device Deep Neural Network for Face Detection," available at https://machinelearning.apple.com/research/face-detection, refers to the text of the article in its entirety, and denies any attempt to paraphrase or characterize the article's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

100. As this diagram demonstrates, the Photos App receives a photograph as input and employs an algorithm that iterates its face detection process in increasingly finer detail in an effort to create a "final prediction of the faces in the image."

ANSWER: Apple admits that this paragraph purports to quote from or paraphrase portions of the November 2017 article "An On-device Deep Neural Network for Face Detection," available at https://machinelearning.apple.com/research/face-detection, refers to the text of the article in its entirety, and denies any attempt to paraphrase or characterize the article's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

101. At minimum, this demonstrates that when Defendant's Photos App utilizes its facial recognition "feature," Defendant collects "biometric information" as defined by BIPA.

ANSWER: Denied.

102. However, Defendant failed to obtain informed written consent prior to collecting this biometric information as required by BIPA.

ANSWER: Denied.

103. In its '952 Patent, Defendant describes a method "for organizing images, such as digital images, by correlating one or more faces represented in the images." U.S. Patent No. 9,977,952 (filed Oct. 31, 2016) at 1:18–20.

ANSWER: Apple admits that it holds U.S. Patent 9,977,952. Apple refers to the text of the patent in its entirety and denies any attempt to paraphrase or characterize the patent's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

104. Defendant explains in the '952 Patent that its invention relates to "[f]acial recognition algorithms." Id. at 1:36–38.

ANSWER: Apple admits that it holds U.S. Patent 9,977,952. Apple refers to the text of the patent in its entirety and denies any attempt to paraphrase or characterize the patent's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

105. On information and belief, Defendant has implemented the methods and embodiments described in the '952 Patent in its Photos App in collecting Biometric Data from Plaintiffs and other Illinois residents.

ANSWER: Apple admits only that it holds U.S. Patent 9,977,952. Apple denies any remaining allegations in this paragraph.

106. Defendant has explained the "advantages" of its automatic collection of biometric identifiers and automatic population of albums by persons in photographs on Apple Devices. One such advantage that Defendant has identified involves helping Apple Device users to understand the functionality of Defendant's Photos App: Organizing images by the people represented in the media provides several potential advantages. For example, such an organizational scheme can be intuitive for users of an image system, enabling users to quickly understand the functioning of the system. Further, the burden of manually organizing many images can be substantially eliminated or reduced. In addition, images can be accurately grouped based on a person represented in the images. Accurately grouping images can provide improved accessibility, organization and usability of the images by users. Id. at 3:4–13.

ANSWER: Apple admits that it holds U.S. Patent 9,977,952. Apple refers to the text of the patent in its entirety and denies any attempt to paraphrase or characterize the patent's complete text and all allegations inconsistent therewith. Apple further admits that it has designed the Photos app to help users find, edit, and share their best shots

(https://apple.com/ios/photos). Apple denies any remaining allegations in this paragraph.

107. Contrary to the requirements of BIPA, Defendant has not, despite its collection of Biometric Data, developed any written policy, made available to the public, establishing a retention schedule or guidelines for permanently destroying Biometric Data.

ANSWER: Apple denies that the Complaint alleges activity to which section 15(a) of BIPA applies and denies the allegations in this paragraph.

108. Consequently, Apple Devices are currently incapable of lawful use in Illinois, because they automatically collect Biometric Data without consent in violation of BIPA, and because the Apple Device user is prohibited by Defendant's EULAs from altering Defendant's software, which Defendant alone owns and controls, to prevent the unlawful collection of the Biometric Data of the user and those whose photographs appear on the user's device.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

109. Defendant intentionally designed and licensed the Apple Devices to be incapable of lawful use in Illinois.

ANSWER: Denied.

110. The primary purpose of the Photo Sorting Software is to identify individuals.

ANSWER: Denied.

111. The identities of people appearing in photos are obtained and derived by Defendant through its software's analysis of data on Apple Devices. This process happens without user involvement or control.

ANSWER: Denied.

112. The Photos Sorting Software does not rely solely on user input to identify people appearing in photographs.

ANSWER: Denied.

113. Rather, the Photos Sorting Software leverages a wide range of information stored on Apple Devices and in the cloud to make suggestions regarding the identity of people appearing in photographs.

ANSWER: Denied.

114. This information includes, but is not limited to, information stored in users' list of personal contacts.

ANSWER: The allegations in this paragraph are vague and ambiguous by virtue of their use of the undefined phrases "[t]his information" and "information stored in users' list of personal contacts." To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

115. Defendant has publicly confirmed that the Photos App "intelligently suggests names from your Contacts or you can enter one yourself."

ANSWER: The allegations in this paragraph are vague and ambiguous by virtue of attributing a quotation to Apple without identifying the source. To the extent an answer is deemed necessary, Apple refers, for illustrative purposes, to https://support.apple.com/en-us/HT207103 for its complete text and denies any attempt to paraphrase or characterize its complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

116. [redacted]

ANSWER: Denied.

117. In the People albums in the Photos App, Apple Devices prompt the user to confirm suggestions that the photograph is of a particular person. This prompt appears as an inline suggestion of the form "Is this X?" as shown in the example below:

ANSWER: Denied.

118. After biometric identifiers are collected and Defendant's software has a sufficient sampling of images, the Photos App applies an algorithm to identify the Apple Device user, thereby creating biometric information.

ANSWER: Denied.

119. [redacted]

ANSWER: Denied.

120. Defendant collects and stores on servers it controls biometric information derived from faceprints that Defendant uses to identify individuals.

ANSWER: Denied.

121. Starting with the release of iOS 11, which was released for public beta testers on June 26, 2017 and to the general public on September 19, 2017, as well as the release of macOS High Sierra, which was released as a public beta on June 29, 2017 and to the general public on September 25, 2017, Defendant began advertising the synchronizing of the "People" album across devices with the iCloud Photo Library (this synchronizing referred to herein as "Faces Sync").

ANSWER: The allegations in this paragraph are vague and ambiguous by virtue of their use of the undefined phrase "released for public beta testers." Apple admits only that iOS 11, which Apple released as a free update on September 19, 2017, and macOS High Sierra, which Apple released as a free update on September 25, 2017, included an optional feature for users to keep their People albums up to date across devices with iCloud Photo Library. Apple denies any remaining allegations in this paragraph or its footnotes.

122. iCloud is a service offered by Defendant for remote storage of user data, i.e., a cloud-based data storage system.

ANSWER: Apple admits only that it provides the iCloud product, software, services, and websites, which permit users to utilize certain Internet services, including storing their personal content and making it accessible on their compatible devices and computers. Apple denies any remaining allegations in this paragraph.

123. iCloud Photo Library ("ICPL") is Defendant's service that stores and synchronizes photographs and associated data, allowing users to access this data from multiple Apple Devices, if those devices are logged into iCloud with the user's Apple ID.

ANSWER: Apple admits only that: (1) iCloud Photos (or iCloud Photo Library) works with the Photos app to keep a user's photos and videos securely stored in iCloud, so the user can access the user's library from compatible devices, if (2) the

user has iCloud Photos enabled and is signed in to iCloud with the same Apple ID on those devices. Apple denies any remaining allegations in this paragraph.

124. Defendant automatically enables iCloud for users running Apple devices with iOS 9 or later who sign in with their Apple ID when they set up the device, unless the user is upgrading the device and has previously chosen not to enable iCloud.

ANSWER: Apple admits that this paragraph paraphrases portions of the "Welcome to iCloud" page on the Apple website (https://www.apple.com/legal/internet-services/icloud/), refers to the text of the page in its entirety, and denies any attempt to paraphrase or characterize the page's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

125. Users can disable iCloud. But when iCloud is enabled, Defendant stores user content on Defendant's or third-party providers' servers.

ANSWER: Apple admits the allegations in the first sentence of this paragraph. Apple admits that the second sentence of this paragraph paraphrases portions of the "Welcome to iCloud" page on the Apple website (https://www.apple.com/legal/internet-services/icloud/), refers to the text of the page in its entirety, and denies any attempt to paraphrase or characterize the page's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

126. The basic tier of iCloud services is free to Apple Device users.

ANSWER: Apple admits that, when a user signs up for iCloud, the user automatically gets 5 gigabytes of free storage. Apple denies any remaining allegations in this paragraph.

127. Defendant states that "[w]ith iCloud Photos, your People album is kept up to date on all your devices that meet" certain "minimum system requirements" and that "[w]hen iCloud Photos is enabled," all of a user's "Memories and People are updated everywhere."

ANSWER: Apple admits that this paragraph purports to quote or paraphrase portions of a webpage on the Apple website appearing at https://support.apple.com/guide/iphone/find-people-in-photos-iph9c7ee918c/ios and a support article appearing at https://support.apple.com/en-us/HT204264, refers to the text of the webpage and support article in their entirety, and denies any attempt to paraphrase or characterize the webpage's or article's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

128. [redacted]

ANSWER: Denied.

129. [redacted]

ANSWER: Denied.

130. [redacted]

ANSWER: Denied.

131. [redacted]

ANSWER: Apple admits only that the Photos app uses cropped versions of photos to create thumbnails for faces, and the user can choose whether to: (1) manually add a name to someone in their People album, (2) confirm or reject photos in a collection, or (3) change the key photo used for the face thumbnail. Apple denies the remaining allegations in this paragraph.

132. [redacted]

ANSWER: Denied.

133. [redacted]

ANSWER: Denied.

134. [redacted]

ANSWER: Denied.

135. [redacted]

ANSWER: Denied.

136. Sync Data is biometric information under the meaning of BIPA because it is derived from biometric identifiers, i.e., faceprints ("scans . . . of facial geometry"), and it is used to identify individuals.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

137. Sync Data is transmitted among users' devices by means of Defendant's servers.

ANSWER: Denied.

138. Sync Data is "collected" by Defendant under the meaning of BIPA.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

139. Sync Data is stored on Defendant's servers.

ANSWER: Denied.

140. Therefore, Defendant possesses Sync Data, under the meaning of BIPA.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

141. Defendant also claims that Photos App data is encrypted and that "[n]o one else can access or read this data." While Defendant assures customers that their data is private and secure, in fact, Defendant stores encryption keys in the cloud. And encryption keys for Photo data have, at all relevant times, been stored by Defendant in escrow such that Defendant has the ability to access encryption keys and therefore photographs, as well as associated Sync Data, if it chooses to do so.

ANSWER: Apple admits that the first and second sentences of this paragraph purport to quote or paraphrase portions of a support article appearing at https://support.apple.com/en-us/HT202303 and legal process guidelines appearing at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf, refers to the text of the article and guidelines in their entirety, and denies any attempt to misstate, paraphrase, or characterize the article's or guidelines' complete text and all allegations inconsistent therewith. The allegations in the third sentence of this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies that the allegations of the Complaint set forth with respect to Plaintiffs or Apple any access to encryption keys, photographs, or Sync Data. Apple denies any remaining allegations in this paragraph.

142. Defendant also uses identities of individuals derived from faceprints of photographic subjects in the Photos App for various other purposes on Apple Devices, without the user's knowledge or the consent of the subject, including suggesting contact names ("Contact Suggestions") and presenting curated "Memories."

ANSWER: Denied.

143. "The Photos app recognizes significant people, places, and events in your library, then presents them in curated collections called Memories."

ANSWER: Apple admits that this paragraph purports to quote or paraphrase portions of a support article appearing at https://support.apple.com/en-us/HT207023, refers to the text of the article in its entirety, and denies any attempt to misstate, paraphrase, or characterize the article's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

144. Defendant, through its software, uses faceprints generated via analysis of photos in the Photos App to suggest contact names in a variety of ways, including by comparing those faceprints to faceprints extracted from FaceTime video calls and from photographs of people in users' list of contacts.

ANSWER: Denied.

145. FaceTime is a proprietary videotelephony product developed by Defendant, available on Apple Devices throughout the relevant time. "When [a user] make[s] or receive[s] a FaceTime call from someone who's not in [the user's] Contacts, FaceTime may make a suggestion about who it is and supply additional contact information so [the user] can create a card for that person." FaceTime makes these suggestions by extracting faceprints from video images of the callers, and comparing those faceprints to the database of identities in users' People albums.

ANSWER: Apple admits that it developed the FaceTime app, which is available for iPhones, iPads, iPod touches, and Macs. Apple further admits that the second sentence of this paragraph purports to quote or paraphrase portions of a page on the Apple website (https://support.apple.com/guide/facetime/add-contacts-while-using-facetime-on-mac-fctm18752901/mac), refers to the text of the page in its entirety, and denies any attempt to misstate, paraphrase, or characterize the article's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

146. "Memories" and "Contact Suggestions" require identification of individual persons in order to function. These features therefore use biometric information as that term is

defined in BIPA, i.e., "information, regardless of how it is captured...based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

ANSWER: Denied.

147. The biometric information embedded in "Memories" and "Contact Suggestions" is stored on iCloud and synced across user devices.

ANSWER: Denied.

148. Defendant does not obtain informed written consent before collecting this biometric information, nor does it publish or comply with any policy regarding the purpose, destruction, or retention of this biometric information.

ANSWER: Apple denies that the Complaint alleges activity to which sections 15(a) or 15(b) of BIPA apply and denies the allegations in this paragraph.

149. [redacted]

ANSWER: Denied.

150. Defendant's terms of use for iCloud states that it may "prescreen, move, refuse, modify and/or remove" any content Apple Device users store.

ANSWER: Apple admits that this paragraph paraphrases portions of the "Welcome to iCloud" page on the Apple website (https://www.apple.com/legal/internet-services/icloud/), refers to the text of the page in its entirety, and denies any attempt to paraphrase or characterize the page's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

151. Defendant reserves the right to and admits to scanning user data stored in iCloud.

ANSWER: Apple admits that the footnote to this paragraph quotes, and the allegations in the paragraph purport to paraphrase, portions of Apple's Privacy Policy appearing at https://www.apple.com/legal/privacy/en-ww/, refers to the text of the Privacy Policy in its entirety, and denies any attempt to paraphrase or characterize the

Privacy Policy's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

152. Defendant recently announced—and then retracted, after a backlash from its users over privacy implications—a plan to scan users' photo libraries for Child Sexual Abuse Material ("CSAM").

ANSWER: The allegations in this paragraph are immaterial and impertinent and, accordingly, should be stricken. Fed. R. Civ. P. 12(f). To the extent an answer is deemed necessary, Apple admits only that: (1) it announced certain Expanded Protections for Children in August 2021 that included a feature for detecting known child sexual abuse material ("CSAM") that was designed to keep CSAM off iCloud Photos without providing information to Apple about any photos other than those that match known CSAM images and (2) this CSAM detection feature was not implemented. Apple denies any remaining allegations in this paragraph.

153. Defendant admitted in public statements that the proposed CSAM monitoring system was built on the ICPL's existing capability that "allow[s] Apple servers to access a visual derivative – such as a low-resolution version – of each matching image" stored on users' Apple Devices. The proposed system would allow "[t]hese visual derivatives . . . [to be] examined by human reviewers who confirm that they are CSAM material, in which case they disable the offending account and refer the account to a child safety organization[.]"

ANSWER: The allegations in this paragraph are immaterial and impertinent and, accordingly, should be stricken. Fed. R. Civ. P. 12(f). To the extent an answer is deemed necessary, Apple admits that this paragraph quotes or paraphrases portions of the Security Threat Model Review of Apple's Child Safety Features appearing at https://www.apple.com/child-safety/pdf/Security_Threat_Model_Review_of_Apple_Child_Safety_Features.pdf, refers to the text of the paper in its entirety, and denies any attempt to misstate, paraphrase, or characterize the paper's complete text

and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

154. Indeed, public reports suggest that Defendant has been scanning iCloud content for at least nearly a decade.

ANSWER: The allegations in this paragraph are immaterial and impertinent and, accordingly, should be stricken. Fed. R. Civ. P. 12(f). To the extent an answer is deemed necessary, Apple admits that this paragraph cites and purports to paraphrase a single third-party article that bears the date November 19, 2012. Apple denies any remaining allegations in this paragraph.

155. Defendant admits that analysis performed to identify CSAM is performed on-device.

ANSWER: The allegations in this paragraph are immaterial and impertinent and, accordingly, should be stricken. Fed. R. Civ. P. 12(f). To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

156. In other words, Defendant has the ability to push software to users' Apple Devices that analyzes locally stored information, retrieves that information, and allows Defendant to view locally stored photographs and associated data.

ANSWER: Denied.

157. Defendant has the ability to, and does, review photographs and related data stored on users' Apple Devices.

ANSWER: Denied.

158. As alleged herein, Defendant collects and stores some user Biometric Data on its servers. Because Defendant owns, operates, and controls these servers, it has exclusive control of their contents. Defendant, moreover, has exclusive control over the process by which Biometric Data is harvested and stored on its servers. Defendant, accordingly, possesses that Biometric Data of Plaintiffs which Defendant collects and causes to be stored on Defendant's servers.

ANSWER: Denied.

159. In addition, Biometric Data of Plaintiffs collected by Apple Devices is stored locally on Apple Devices. Defendant possesses data stored locally on Apple Devices because it has

complete and exclusive control over this Biometric Data. To be clear, Defendant controls: Whether biometric identifiers are collected; What biometric identifiers are collected; The type of Biometric Data that are collected and the format in which they are stored; The facial recognition algorithm that is used to collect Biometric Data; What Biometric Data are saved; Whether biometric identifiers are used to identify users (creating biometric information); Whether Biometric Data are kept locally on users' Apple Devices; Whether Biometric Data are encrypted or otherwise protected; and How long Biometric Data are stored.

ANSWER: Denied.

160. The user of an Apple Device has no ability to control the Biometric Data on the user's Apple Device.

ANSWER: Denied.

161. The user has no control over whether Biometric Data is collected from the user's photo library.

ANSWER: Denied.

162. On Defendant's iPhone and iPad devices, the Photos App automatically collects biometric identifiers while running in the background.

ANSWER: Denied.

163. On Macintosh computers, the Photos App collects biometric identifiers from a user's image library as soon as the Photos App is opened.

ANSWER: Denied.

164. Users cannot disable the collection of Biometric Data, cannot limit what information is collected or from whom information is collected, cannot remove the People folder, and cannot delete the database of facial recognition information that Defendant creates or any information in that database.

ANSWER: Denied.

165. Indeed, Defendant's EULAs specifically prohibit users from modifying Defendant's software to prevent the collection of Biometric Data.

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the meaning of "Defendant's EULAs." Apple admits only that this paragraph cites the iOS 13 and iPadOS 13 SLA, refers to the text of the iOS 13 and iPadOS 13 SLA in its entirety, and denies any attempt to paraphrase or characterize the license's

complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

166. Defendant only allows users to use Apple Devices on the condition that Defendant collects Biometric Data.

ANSWER: Denied.

167. Defendant fully controls the Biometric Data on Apple Devices, and therefore possesses it because, for among other reasons, Defendant forbids users from disabling the Biometric Data collection of Apple Devices.

ANSWER: Denied.

168. Defendant profits from the Biometric Data collected by Apple Devices through the sale of those devices.

ANSWER: Apple denies that the Complaint alleges activity to which section 15(c) of BIPA applies and denies the allegations in this paragraph.

169. Defendant uses the face recognition "feature" of its Photos App in order to advertise its operating systems and Apple Devices to potential users.

ANSWER: The allegations in this paragraph are vague and ambiguous by virtue of their use of the undefined phrase "face recognition." Apple admits only that it publicly promotes the various benefits of the Photos app, which is built into certain operating systems for certain devices designed by Apple. Apple denies any remaining allegations in this paragraph.

170. Defendant advertises its Photos App as being able to "recognize the people, scenes, and objects in [photographs]," and that it "uses advanced computer vision to scan all of your photos" so that users can "[s]ort your images by your favorite subjects — the people in your life." Defendant also advertises that users have the ability "to find the exact photos you're looking for, based on who you were with or where you were when you took them."

ANSWER: Apple admits that this paragraph purports to quote or paraphrase portions of a support article appearing at https://support.apple.com/en-us/HT207103, and Photos app webpage appearing at https://www.apple.com/ios/photos, refers to the text

of the support article and webpage in their entirety, and denies any attempt to paraphrase or characterize the article's or webpage's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph.

171. Defendant developed these "features" for its Photos App to compete with similar features being offered on other devices, giving Defendant a competitive edge that allowed Defendant to profit from the sale of Apple Devices.

ANSWER: Apple admits that: (1) there are developers of software applications for the storage of photos other than Apple, (2) there are manufacturers of "other devices," (3) that Apple's products and services face competition, and (4) that Apple is a for-profit corporation. Apple denies any remaining allegations in this paragraph.

172. Indeed, Defendant's public statements regarding its "commitment to privacy" have been picked up by media outlets and others as a justification for the higher prices Defendant charges for its devices.

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

173. For the reasons set forth above, among others, Defendant profits from Biometric Data.

ANSWER: Denied.

174. Defendant is prohibited from profiting from any "person's or . . . customer's biometric information" because Defendant is "a private entity in possession of a biometric identifier." 740 ILCS 14/15(c). Therefore, the fact that Defendant profits from the Biometric Data it collects is unlawful.

ANSWER: Apple denies that the Complaint alleges activity to which section 15(c) of BIPA applies and denies the allegations in this paragraph.

175. Defendant has failed to comply with BIPA's requirements concerning the collection and possession of Biometric Data. With respect to its collection of Biometric Data, Defendant failed to: (1) inform the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored; (2) inform the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used;

or (3) receive a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative. 740 ILCS 14/15(b).

ANSWER: Apple denies that the Complaint alleges activity to which section 15(b) of BIPA applies and denies the allegations in this paragraph.

176. With respect to its possession of Biometric Data, Defendant failed to: develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. 740 ILCS 15(a).

ANSWER: Apple denies that the Complaint alleges activity to which section 15(a) of BIPA applies and denies the allegations in this paragraph.

177. Defendant's failure to comply with BIPA extends to nonusers of its devices. This is because Defendant's Photos App collects and possesses the Biometric Data of everyone who appears in images stored on a user's Apple Device.

ANSWER: Denied.

178. Defendant does not have commercial relationships with the nonusers whose Biometric Data it collects, and does not know which nonusers' Biometric Data it is collecting. Therefore, Defendant cannot obtain informed written consent from nonusers.

ANSWER: Apple denies that it collects biometric data in connection with the Photos app. Apple further denies that the Complaint alleges activity to which BIPA applies. Apple admits only that it does not know and does not attempt to ascertain who appears in a user's photos. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

179. Furthermore, many of the nonusers from whom Defendant collects Biometric Data are minors who cannot give informed written consent.

ANSWER: Apple denies that it collects biometric data in connection with the Photos app. Apple further denies that the Complaint alleges activity to which BIPA applies.

Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

180. Defendant also does not comply with BIPA's prohibition on profiting from Biometric Data.

ANSWER: Denied.

181. Defendant developed the facial recognition feature of its Photos App in part to compete with other electronic device vendors and software developers, and in order to sell Apple Devices.

ANSWER: The allegations in this paragraph are vague and ambiguous by virtue of their use of the undefined phrase "facial recognition." Apple admits that: (1) there are "other electronic device vendors and software developers," (2) that Apple's products and services face competition, and (3) that Apple is a for-profit corporation. Apple denies any remaining allegations in this paragraph.

182. Defendant did, in fact, profit from the sale of Apple Devices as a result of Defendant's facial recognition "feature."

ANSWER: The allegations in this paragraph are vague and ambiguous by virtue of their use of the undefined phrase "facial recognition." Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

183. Defendant's BIPA violations present an imminent threat of serious harm to Plaintiffs and the proposed class.

ANSWER: Denied.

184. When Biometric Data is stored on personal electronic devices, persons from whom Biometric Data has been collected face a multiplicity of threats.

ANSWER: Apple denies that the allegations of the Complaint set forth any biometric data stored on personal electronic devices or persons from whom biometric data has been collected. Apple lacks knowledge or information sufficient to form a belief as to

the unspecified "multiplicity of threats" to which this paragraph refers and therefore denies any remaining allegations in this paragraph.

185. Defendant does not delete the Biometric Data it collects, which are located on numerous devices in this State. Moreover, an Apple Device user's Biometric Data may be stored on one or more iPhones, iPads or MacBooks, as well as discarded Apple Devices. Furthermore, nonusers' Biometric Data that Defendant collects may be stored on one or more Apple Devices.

ANSWER: Apple denies that it collects biometric data in connection with the Photos app. Apple further denies that the allegations of the Complaint set forth any biometric data stored on iPhones, iPads, Mac computers, or discarded devices. Apple lacks knowledge or information sufficient to form a belief as to what a user chooses to store on (and how he or she chooses to use) his or her own device and therefore denies the remaining allegations in this paragraph.

186. For example, an Illinois resident's Biometric Data may be stored on the Apple Devices of his or her family, his or her relatives, his or her friends, his or her coworkers, and anyone else who photographed him or her using an Apple Device.

ANSWER: Apple denies that it collects biometric data in connection with the Photos app. Apple further denies that the allegations of the Complaint set forth any biometric data stored on iPhones, iPads, or Mac computers. Apple lacks knowledge or information sufficient to form a belief as to what a user chooses to store on (and how he or she chooses to use) his or her own device and therefore denies the remaining allegations in this paragraph.

187. Apple Device users cannot prevent their devices from collecting their unique and sensitive Biometric Data, and nonusers cannot control whether Apple Devices containing this unique and sensitive information are lost, stolen, discarded improperly, given to vendors for repair work, or recycled. Nonusers likewise cannot control whether their Biometric Data is extracted, decrypted, or sold.

ANSWER: Apple denies that it collects biometric data in connection with the Photos app. Apple further denies that the allegations of the Complaint set forth any biometric

data stored on iPhones, iPads, or Mac computers. Apple also denies that "Apple Device users cannot prevent their devices from collecting their unique and sensitive Biometric Data." Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph.

188. Information stored in a central location, such as a server, presents a single breach threat. A sophisticated entity may take measures to securely and centrally store information, guarding against the threat of a data breach. By contrast, as the result of the fact that the Biometric Data that Defendant collects are stored on numerous devices, Plaintiffs and members of the Class face the imminent threat of disclosure of their Biometric Data as a result of a data breach on any one of the Apple Devices on which their Biometric Data are stored.

ANSWER: Apple denies that it collects or stores biometric data in connection with the Photos app. Apple further denies that the allegations of the Complaint set forth any biometric data stored on iPhones, iPads, or Mac computers. Apple denies the allegations in the third sentence of this paragraph. Apple lacks knowledge or information sufficient to form a belief as to the unspecified "breach threat" or "measures to securely and centrally store information" to which this paragraph refers and therefore denies all remaining allegations in this paragraph.

189. Defendant has greater than a 40% market share of the smartphone market in the United States, around 10% of the laptop market, and approximately 17% of the desktop market. 96% of adult Americans use smartphones and approximately 75% percent of Americans own a desktop or laptop.

ANSWER: Apple lacks knowledge or information sufficient to form a belief as to the truth of the allegations in this paragraph and therefore denies the same.

190. Many of the Apple Devices used in this State have collected the Biometric Data of multiple individuals other than the Apple Device user. Consequently, numerous Illinois residents have their Biometric Data stored on one or more Apple Devices outside their control.

ANSWER: Apple denies that it collects biometric data in connection with the Photos app. Apple further denies that the allegations of the Complaint set forth any biometric data stored on iPhones, iPads, or Mac computers. Apple lacks knowledge or

information sufficient to form a belief as to what a user chooses to store on (and how he or she chooses to use) his or her own device and therefore denies the remaining allegations in this paragraph.

191. The durability of the memory in Apple Devices creates a nearly permanent risk of a data breach of biometric identifiers and information for both device users as well as nonusers whose Biometric Data have been collected. Apple Devices utilize solid state memory, which can withstand drops, extreme temperatures, and magnetic fields. Unless corrupted, this solid state memory and the information it contains can last in perpetuity. Thus, the Biometric Data on Apple Devices will likely outlast the device battery, the functionality of the device screen, and the natural life of the device user.

ANSWER: Apple admits that certain Apple devices utilize solid state disk storage. Apple denies the remaining allegations in this paragraph.

192. Apple Devices, like all computing devices, are vulnerable to hackers and other malicious bad actors. For example, the Washington Post recently reported that security researchers discovered a "'sustained' . . . and indiscriminate campaign to hack iPhones through certain websites, allowing attackers to steal messages, files and track location data every 60 seconds." Just days prior to that report's publication, Defendant released an "emergency fix" to a different vulnerability that allowed "malicious hackers to take control of all Apple desktop and laptop computers [and] mobile devices."

ANSWER: Apple admits that unknown parties may seek to exploit security issues in electronic devices. Apple further admits that it periodically has released operating system upgrades related to security issues and that iOS 12.4.1 provided important security and stability updates. Apple refers to the Apple security updates webpage, available at https://support.apple.com/en-us/HT201222, which lists security updates for Apple software. Apple denies any remaining allegations in this paragraph.

193. Biometric Data may persist on discarded Apple Devices, which could be extracted by malicious actors using methods of removal that may or may not currently exist. The risk of illicit harvesting of biometric information from discarded Apple Devices therefore extends far into the future.

ANSWER: Apple denies that it collects biometric data in connection with the Photos app. Apple further denies that the allegations of the Complaint set forth any biometric

data stored on iPhones, iPads, Mac computers, or discarded devices. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

194. Defendant is directly liable for the BIPA violations based on the functionality of its proprietary software, which it wholly owns and exclusively controls, and which Apple Device users are prohibited from owning, controlling, or modifying.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

*195. Furthermore, Defendant is vicariously liable for BIPA violations because its software operated as a "software agent:" A software agent is essentially a software version of a concept familiar in the law: an entity that performs a task, with some degree of autonomy, on behalf of someone else. An agent in the physical world can perform its task without input from the principal; this is equally true when an agent is a machine, such as a robot on a factory floor, which can perform its repetitive task without needing constant human guidance. A software agent operates in the same way—it can perform its task without human input. For example, a software agent useful to shoppers could scan a large number of websites for a certain product, and identify the website offering the product at the lowest price; to the text of the note without such a program, the human user would have to look at each website herself. NetFuel, Inc. v. F5 Networks, Inc., No. 13-7895, 2017 WL 2834538, at *1 (N.D. Ill. June 29, 2017); see also Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005) (technology distributor contributorily and vicariously liable for the unlawful use of technology where the technology has an "unlawful objective"); Akamai Techs., Inc. v. Limelight Networks, Inc., 797 F.3d 1020, 1024 (Fed. Cir. 2015) (software designer liable for infringing conduct of software where use of software "conditioned" on infringing behavior); Shaw v. Toshiba Am. Info. Sys., Inc., 91 F. Supp. 2d 926 (E.D. Tex. 1999) (software designer liable for harm to third party caused by software).*

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple admits that this paragraph quotes or paraphrases selected portions of various judicial opinions, reserves all arguments with regard to those judicial opinions, and otherwise denies the allegations in this paragraph.

196. In this case, Defendant, in addition to being directly liable, is also vicariously liable for BIPA violations caused by the use of Apple Devices because, under principles of agency law, Defendant's Apple Devices functioned as software agents subject to the actual authority of

Defendant, because Defendant acted negligently in controlling its proprietary software installed on Apple Devices, or both. Restatement (Third) Of Agency §§ 7.04; 7.05 (2006).

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

197. Further, Defendant is vicariously liable because the use of its Apple Devices was conditioned on unlawful use and had an objective that was unlawful under Illinois law.

ANSWER: The allegations in this paragraph consist of legal conclusions and argument to which no answer is required. To the extent an answer is deemed necessary, Apple denies the allegations in this paragraph.

198. Each Plaintiff has used one or more Apple Device to take or store photographs of themselves and other people. No Plaintiff was aware Defendant's facial recognition technology would collect Biometric Data and organize photographs based on facial geometries. However, Defendant's facial recognition technology has collected Biometric Data not only from Plaintiffs, but also from individuals appearing in photographs on Plaintiffs' Apple Devices, including parents, grandchildren, siblings, cousins, friends, and/or co-workers of Plaintiffs.

ANSWER: Apple denies that the Photos app collects biometric data. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

199. Plaintiff Jane Doe is an eight-year-old minor. She owns an iPad, which she has used to take photos, including of herself. She also appears in the photographs of her relatives who own various Apple products. She has not, and cannot, give consent for her biometric information to be collected or possessed by Defendant. Further, Jane Doe's parents have not given informed written consent to allow Defendant to collect or possess Jane Doe's Biometric Data. The People and Places "feature" of the Photos App on Jane Doe's iPad has automatically generated a photo album that contains photographs of Jane Doe based on Defendant's collection of her Biometric Data.

ANSWER: Apple denies that it or the Photos app collects or uses biometric data as alleged herein. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

200. Plaintiff Richard Robinson has owned an iPhone for several years. Mr. Robinson also has previously owned an iPad. Mr. Robinson has taken photos with his iPhone, including of himself and other family members. Although he has "tagged" individuals in the photographs that Defendant has organized by facial geometry, Mr. Robinson is unsure whether he has ever actually used Defendant's People and Places "feature" in the Photos App, and has never provided consent, let alone informed written consent, for his Biometric Data to be used or collected. Nevertheless, the People and Places feature in the Photos App on his iPhone has created various albums for individuals appearing in his photographs: The above screenshot is from Mr. Robinson's iPhone and shows the people-specific albums automatically generated by Defendant's software. From left to right, top to bottom, the albums in the above screenshot correspond to Mr. Robinson's wife, daughter-in-law, brother, daughter, himself, and granddaughter.

ANSWER: Apple denies that it or the Photos app collects or uses biometric data as alleged herein. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

201. Plaintiff Yolanda Brown has had an iPhone for several years, and has taken various photographs throughout that period. The earliest photos of herself that are currently stored on her iPhone date from approximately ten years ago. She was not aware of Defendant's People and Places "feature" of the Photos App, though she has "tagged" individuals in the photographs that Defendant has organized by facial geometry. The People and Places feature of the Photos App on Ms. Brown's phone has automatically generated photo albums for photographs containing each of her three nieces, six aunts, five cousins, and brother. Ms. Brown never consented to Defendant's collection of her Biometric Data.

ANSWER: Apple denies that it or the Photos app collects or uses biometric data as alleged herein. Apple lacks knowledge or information sufficient to form a belief as to the truth of the remaining allegations in this paragraph and therefore denies the same.

202. Defendant applies its facial recognition technology to every picture that a user saves on his or her Apple Device running Defendant's Photos App.

ANSWER: Denied.

203. When an Illinois resident purchases an Apple Device, Defendant does not inform them that Biometric Data will be collected from every person whose picture is stored on the device, including the Apple Device user and any other person whose face appears in a photograph stored on the Photos App. Defendant has not informed Plaintiffs that Biometric Data has been and is being collected from the individuals whose faces appear in photographs stored on users' Photos Apps.

ANSWER: Apple denies that it or the Photos app collects biometric data as alleged herein. Apple further denies that the Complaint alleges activity to which BIPA applies and denies that Apple has violated any obligation under BIPA. Apple denies any remaining allegations in this paragraph.

204. Moreover, Defendant has not informed Plaintiffs that the Photos App is installed on their devices by default and will operate on mobile devices whenever a photograph is added to the Photos App or when the Photos App is started on laptop or desktop computers.

ANSWER: Denied.

205. As a result, Defendant did not obtain consent from Plaintiffs in any form prior to collecting their facial geometry data, let alone written, informed consent as required by BIPA. Nor has Defendant obtained consent from other members of the proposed class, including minors whose photos appear in the Photos App.

ANSWER: Apple denies that it collects biometric data in connection with the Photos app. Apple further denies that the Complaint alleges activity to which BIPA applies, denies that Apple has violated any obligation under BIPA, and denies that this action may be maintained individually or on behalf of any class. Apple denies any remaining allegations in this paragraph.

206. Defendant has collected biometric information and biometric identifiers from Plaintiffs in violation of BIPA.

ANSWER: Denied.

207. Plaintiffs seek to represent the following similarly situated individuals (collectively, the "Class"): Subclass 1: All Illinois citizens whose faces appeared in one or more photographs taken or stored on their own Apple Devices or whose faces appeared in one or more photographs stored in their iCloud Photos Library from September 13, 2016 until present. Subclass 2: All Illinois citizens whose faces appeared in one or more photographs taken or stored on an Apple Device other than their own or whose faces appeared in one or more photographs stored in an iCloud Photos Library other than their own from September 13, 2016 until present.

ANSWER: Apple admits that Plaintiffs purport to bring this action on behalf of themselves and two subclasses that Plaintiffs define in this paragraph. Apple denies

any remaining allegations in this paragraph and states that this action cannot be maintained individually or on behalf of any class.

208. Numerosity. The Class includes thousands of people, such that it is not practicable to join all Class members into one lawsuit.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies any allegations in this paragraph and states that this action cannot be maintained individually or on behalf of any class.

209. Commonality. The issues involved with this lawsuit present common questions of law and fact, including: whether Defendant collected and/or possessed the Class's biometric identifiers or biometric information; whether Defendant profited from biometric identifiers or biometric information; whether Defendant properly informed Class members that it captured, collected, used, and stored their biometric identifiers and/or biometric information; whether Defendant obtained "informed written consent" (740 ILCS 14/10) to capture, collect, use, and store Class members' biometric identifiers and/or biometric information; whether Defendant used Class members' biometric identifiers and/or biometric information to identify them; and whether Defendant' violations of BIPA were committed recklessly or negligently.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies any allegations in this paragraph and states that this action cannot be maintained individually or on behalf of any class.

210. Predominance. The common questions of law and fact predominate over any individual issue that may arise on behalf of an individual Class member.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies any allegations in this paragraph and states that this action cannot be maintained individually or on behalf of any class.

211. Typicality. Plaintiffs, the members of the Class, and Defendant have a commonality of interest in the subject matter of the lawsuit and the remedy sought.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies any allegations in this paragraph and states that this action cannot be maintained individually or on behalf of any class.

*212. Adequacy. Plaintiffs and counsel will fairly and adequately protect the interests of Class members. Plaintiffs' counsel, Schlichter Bogard & Denton, LLP, will fairly and adequately represent the interests of the Class. Schlichter Bogard & Denton, LLP has a well-documented track record of serving as class counsel in this State and elsewhere. Schlichter Bogard & Denton's pioneering work in class actions brought on behalf of citizens of this State and others has been covered by numerous national publications, including the New York Times and Wall Street Journal, among other media outlets. By way of limited example, courts in this State have noted in reference to the work of Schlichter Bogard & Denton, LLP in class action litigation: "This Court is unaware of any comparable achievement of public good by a private lawyer in the face of such obstacles and enormous demand of resources and finance." Order on Attorney's Fees, Mister v. Illinois Central Gulf R.R., No. 81-3006 (S.D. Ill. 1993). "This Court finds that Mr. [Jerome J.] Schlichter's experience, reputation and ability are of the highest caliber. Mr. Schlichter is known well to the District Court Judge and this Court agrees with Judge Foreman's review of Mr. Schlichter's experience, reputation and ability." Order on Attorney's Fees, Wilfong v. Rent-A-Center, No. 0068-DRH (S.D. Ill. 2002). "Class Counsel performed substantial work . . . investigating the facts, examining documents, and consulting and paying experts to determine whether it was viable. This case has been pending since September 11, 2006. Litigating the case required Class Counsel to be of the highest caliber and committed to the interests of the [class]." Will v. General Dynamics, No. 06-698, 2010 WL 4818174, at *2 (S.D. Ill. Nov. 22, 2010). "Schlichter, Bogard & Denton has achieved unparalleled results on behalf of its clients, . . . has invested . . . massive resources and persevered in the face of . . . enormous risks[.]" Nolte v. Cigna Corp., No. 07-2046, 2013 WL 12242015, at *2 (C.D. Ill. Oct. 15, 2013). "Litigating this case against formidable defendants and their sophisticated attorneys required Class Counsel to demonstrate extraordinary skill and determination." Beesley v. Int'l Paper Co., No. 06-703, 2014 WL 375432, at *2 (S.D. Ill. Jan. 31, 2014). "Schlichter, Bogard & Denton demonstrated extraordinary skill and determination in obtaining this result for the Class." Abbott v. Lockheed Martin Corp., No. 06-701, 2015 WL 4398475, at *2 (S.D. Ill. July 17, 2015). Plaintiffs' counsel Christian Montroy is also an experienced class action practitioner who will adequately represent the Class.*

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies any allegations in this paragraph and states that this action cannot be maintained individually or on behalf of any class.

213. *Superiority. A class action is the appropriate vehicle for fair and efficient adjudication of Plaintiffs' and Class members' claims because if individual actions were required*

to be brought by each member of the Class, the result would be a multiplicity of actions, creating a hardship to the Class, to the Court, and to Defendant.

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies any allegations in this paragraph and states that this action cannot be maintained individually or on behalf of any class.

COUNT I—VIOLATION OF 740 ILCS 14/15(c)

214. Plaintiffs incorporate paragraphs 1 through 213 as though fully realleged herein.

ANSWER: Apple incorporates the foregoing answers to paragraphs 1 through 213 as though fully reasserted herein.

215. Under BIPA, Defendant owed a duty to Plaintiffs and the Class not to profit from their Biometric Data. See 740 ILCS 14/15(c).

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple refers to BIPA for its complete text and denies any attempt to paraphrase or characterize BIPA's complete text and all allegations inconsistent therewith. Apple denies any remaining allegations in this paragraph and further states that the Complaint fails to state a claim against Apple.

216. Defendant is subject to BIPA section 15(c) because it is a "private entity in possession of a biometric identifier or biometric information."

ANSWER: The allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies such allegations and further states that the Complaint fails to state a claim against Apple.

217. Defendant possesses the Biometric Data stored locally on the electronic devices of Plaintiffs and the Class because, as alleged herein, Defendant exclusively controls that Biometric Data.

ANSWER: Denied.

218. In addition, on information and belief, Defendant possesses, among other Biometric Data, scans of facial geometry that are stored on devices owned by Defendant. This includes, but is not limited to, scans of facial geometry that are present on devices owned by Defendant, including those used by employees of Defendant.

ANSWER: The allegations in this paragraph are immaterial and impertinent and, accordingly, should be stricken. Fed. R. Civ. P. 12(f). Additionally, the allegations in this paragraph consist of legal conclusions to which no answer is required. To the extent an answer is deemed necessary, Apple denies such allegations and further states that the Complaint fails to state a claim against Apple.

219. Defendant violated BIPA section 15(c) by profiting from Plaintiffs' and Class members' biometric identifiers and biometric information, including scans of facial geometry and related biometric information, by, among other things, marketing and selling its devices based upon claims of their ability to sort photographs, as alleged in more detail herein.

ANSWER: Denied.

220. Defendant's BIPA violations are violations of Defendant's duty of ordinary care owed to Plaintiffs and the Class.

ANSWER: Denied.

221. In the alternative, Defendant's BIPA violations were willful and wanton. Defendant knowingly, intentionally and/or recklessly violated the duty it owed to Plaintiffs and the Class.

ANSWER: Denied.

222. Plaintiffs incurred injuries that were proximately caused by Defendant's conduct. Through its actions, Defendant exposed Plaintiffs and the Class to imminent threats of serious harm.

ANSWER: Denied.

223. Plaintiffs in this Count I hereby request the relief set forth in the Prayer for Relief below, and incorporated as though fully set forth herein.

ANSWER: Apple denies that the Complaint states a claim against Apple. Apple further denies that Plaintiffs may seek any relief stated in this paragraph. Apple denies any remaining allegations in this paragraph.

PRAYER FOR RELIEF WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, pray for judgment against Defendant Apple Inc. as follows: A. Certifying this case as a class action, appointing Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class counsel; B. Finding that Defendant's conduct violates BIPA; C. Awarding actual damages caused by Defendant's BIPA violations; D. Awarding statutory damages of $5,000 for each intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), and damages of $1,000 for each negligent violation pursuant to 740 ILCS 14/20(1); E. Awarding injunctive and/or other equitable or non-monetary relief as appropriate to protect the Class, including by enjoining Defendant from further violating BIPA pursuant to 740 ILCS 14/20(4); F. Awarding Plaintiffs reasonable attorneys' fees, costs, and other litigation expenses pursuant to 740 ILCS 14/20(3); G. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable; and H. Awarding such other and further relief as this Court deems appropriate and as equity and justice may require.

ANSWER: Apple denies the allegations in Plaintiffs' *ad damnum* and requests that judgment be entered for Apple and against Plaintiffs in this action.

JURY DEMAND Plaintiffs request trial by jury of all claims asserted herein.

ANSWER: Apple admits that Plaintiffs demand a trial by jury and likewise demands a jury trial as to all matters so triable.

AFFIRMATIVE DEFENSES

Without admitting the sufficiency of Plaintiffs' allegations and without assuming any burden of proof not placed on it by applicable law, Apple asserts the following affirmative defenses. Apple expressly reserves the right to amend its affirmative defenses at any time, including and up to and at trial, based on all further investigations, discovery, and preparation for the trial of this action.

FIRST AFFIRMATIVE DEFENSE: Unconstitutionality of BIPA/Commerce Clause

Plaintiffs' claims are barred in whole or in part by the Dormant Commerce Clause of the United States Constitution. If the conduct alleged in the Complaint qualifies as a violation of BIPA,

then BIPA would: (1) have the practical effect of allowing Illinois law to regulate conduct occurring entirely outside of Illinois; (2) subject Apple to inconsistent statutes and regulations; and (3) usurp the prerogative of other states to make their own policy choices and to apply their own laws.

SECOND AFFIRMATIVE DEFENSE:
Unconstitutionality of BIPA/Due Process

Plaintiffs' claims are barred in whole or in part by the Due Process Clauses of the Fifth and Fourteenth Amendments to the United States Constitution. The Photos app does not use or rely on biometric identifiers or biometric information, and the review and grouping of photos by the Photos app occurs entirely on Plaintiffs' devices, which are not in Apple's possession, custody, or control. In addition, Apple does not and cannot use the Photos app to identify an individual.

BIPA does not outlaw the creation or use of biometric identifiers or biometric information. To the contrary, section 5 of BIPA is clear that the legislature intended to promote the development of technologies and transactions that rely on biometric data. Nothing in the text of the legislative history of BIPA evinces any legislative intent to regulate manufacturers of devices or developers of software, as opposed to the private entities who actually possess, store, collect, purchase, receive through trade, otherwise obtain, disclose, redisclose, or disseminate biometric identifiers and biometric information. Furthermore, the legislative history of BIPA shows that the legislature intended to regulate only biometric identifiers and biometric information when used or capable of being used to identify an individual.

Finally, the definitions and provisions of BIPA are vague and ambiguous as applied to Apple and the Photos app because they fail to provide a person of ordinary intelligence fair notice of what they prohibit and are so standardless that they authorize or encourage seriously discriminatory and unfair enforcement without notice.

Accordingly, Apple did not have fair notice that 740 ILCS 14/15 could be applied in the manner in which Plaintiffs allege here, and as applied in this case, BIPA violates the Due Process Clauses of the Fifth and Fourteenth Amendments to the United States Constitution.

THIRD AFFIRMATIVE DEFENSE:
Unconstitutionality of BIPA/Excessive Fines

Plaintiffs' claims are barred in whole or in part by the Due Process Clause of the Fourteenth Amendment to the United States Constitution. Upon information and belief, Plaintiffs and the putative class members whom they purport to represent have not suffered any actual damages as a result of the conduct alleged in the Complaint. The Complaint, however, requests statutory damages in the amount of $1,000 or $5,000 per violation, for Plaintiffs individually and for members of the putative class. The statutory damages amounts are unreasonable, grossly excessive, and disproportionate to any injury suffered by Plaintiffs or by members of the putative class. Accordingly, as applied in this case, both on behalf of Plaintiffs individually and on behalf of the alleged putative class, the statutory damages under 740 ILCS 14/20 violate the Due Process Clause of the Fourteenth Amendment to the United States Constitution.

FOURTH AFFIRMATIVE DEFENSE:
Unconstitutionality of BIPA/Free Speech

Plaintiffs' claims are barred in whole or in part by the Free Speech Clause of the First Amendment to the United States Constitution. If the conduct alleged in the Complaint qualifies as a violation of BIPA, then BIPA would restrict speech or inherently expressive conduct, including the taking of photos and grouping those photos into collections by their contents.

The Photos app does not use or rely on biometric identifiers or biometric information; the review and grouping of photos by the Photos app occurs entirely on devices in Plaintiffs' possession, custody, and control; and Apple does not access or obtain—or seek to access or obtain—Plaintiffs' photos or People albums. Rather, Plaintiffs seek to apply BIPA, in this case, to

restrict the automated creation of People albums on Plaintiffs' devices in violation of the First Amendment (applicable through the Fourteenth Amendment) to the United States Constitution.

FIFTH AFFIRMATIVE DEFENSE:
Consent

Plaintiffs' claims are barred in whole or in part because Plaintiffs and the putative class members whom they purport to represent, or individuals with authority to act on their behalf, consented to the conduct alleged to violate BIPA.

SIXTH AFFIRMATIVE DEFENSE:
Waiver

To the extent that a plaintiff or alleged member of the putative class has started or continued to use the Photos app after the filing of this Complaint or reading any public article on which the Complaint is based—whichever occurred first—their claims are barred, in whole or in part, by the doctrine of waiver.

SEVENTH AFFIRMATIVE DEFENSE:
Statute of Limitations

No damages or other relief can be recovered by Plaintiffs and/or members of the asserted putative class to the extent Plaintiffs' claims are barred, in whole or in part, by an applicable contract provision and/or statute of limitations. *See, e.g.*, 735 ILCS 5/13-201 (one-year limitations period for privacy actions); 735 ILCS 5/13202 (two-year limitations period to recover a statutory penalty); 735 ILCS 5/13-205 (five-year limitations period for "all civil actions not otherwise provided for"). Upon information and belief, Apple alleges that Plaintiffs and/or members of the asserted putative class failed to bring the claim remaining before this Court within the period required by the statutes of limitations. Apple also reserves all rights regarding the inapplicability of Illinois law in this matter.

EIGHTH AFFIRMATIVE DEFENSE:
No Extraterritorial Application of BIPA

Plaintiffs' claims are barred in whole or in part because Plaintiffs' interpretation of BIPA would require an impermissible extraterritorial application of BIPA.

NINTH AFFIRMATIVE DEFENSE:
Failure to Mitigate

Plaintiffs' claims are barred in whole or in part by Plaintiffs' failure to take reasonable steps to mitigate their damages. According to the Complaint, Plaintiffs have known, or were reasonably informed, that they could remove photos from their devices at any time. Upon information and belief, Plaintiffs continue to use the Photos app and the People album and have not removed the photos from their devices. Accordingly, Plaintiffs failed to take reasonable steps to mitigate their damages and their claims are barred.

TENTH AFFIRMATIVE DEFENSE:
Estoppel, Laches, and Unclean Hands

Plaintiffs' claims are barred in whole or in part by estoppel, laches, unclean hands, or other equitable defenses. Upon information and belief, including based on Plaintiffs' allegations, Plaintiffs and/or members of the asserted putative class voluntarily operated their own devices and never objected to the conduct alleged in the Complaint before the filing of this lawsuit.

ELEVENTH AFFIRMATIVE DEFENSE:
No Liability for Plaintiffs' Conduct or for Third-Party Acts

Plaintiffs' claims are barred to the extent any alleged damages or injury to Plaintiffs and/or members of the asserted putative class are based on their own conduct or the conduct of third parties.

TWELFTH AFFIRMATIVE DEFENSE:
No Class Action

Plaintiffs' claims on behalf of themselves and the alleged putative class are not appropriate for class treatment, and no class can be certified, because—among other things—BIPA is inapplicable; individual issues predominate; and Plaintiffs are not adequate representatives of, and should be barred from acting on behalf of, the alleged class.

DEFENDANT'S PRAYER FOR RELIEF

WHEREFORE, Apple prays for the following relief:

1. That Plaintiffs recover nothing by reason of their Complaint, and that judgment be rendered in favor of Apple;

2. That Plaintiffs be denied class certification;

3. That Apple be awarded its costs of suit incurred in defense of this action, including reasonable attorneys' fees; and

4. For other such relief as the Court deems proper.

Dated: November 11, 2022

Respectfully Submitted,

Apple Inc.

By: /s/ *Raj Shah*
One of its attorneys

Russell K. Scott (ARDC # 02533642)
Greensfelder Hemker & Gale PC
12 Wolf Creek Drive, Suite 100
Belleville, Illinois 62226
rks@greensfelder.com

Raj N. Shah (ARDC # 06244821)
Eric M. Roberts (ARDC # 6306839)
Matthew J. Freilich (ARDC # 6332688)
DLA Piper LLP (US)
444 West Lake Street, Suite 900
Chicago, Illinois 60606
raj.shah@dlapiper.com
eric.roberts@dlapiper.com
matthew.freilich@dlapiper.com

Isabelle L. Ord*
DLA Piper LLP (US)
555 Mission Street, Suite 2400
San Francisco, California 94105
isabelle.ord@dlapiper.com

* motion to appear *pro hac vice* forthcoming

Certificate of Service

I hereby certify that on November 11, 2022, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system. I further certify that I caused a true and correct copy of the foregoing document to be served by electronic mail on the following attorneys of record:

Jerome J. Schlichter
jschlichter@uselaws.com
Andrew D. Schlichter
aschlichter@uselaws.com
Alexander L. Braitberg
abraitberg@uselaws.com
Nathan H. Emmons
nemmons@uselaws.com
Schlichter Bogard & Denton, LLP
100 South Fourth Street, Suite 1200
St. Louis, MO 63102

Christian G. Montroy
cmontroy@montroylaw.com
Montroy Law Offices, LLC
2416 North Center
P.O. Box 369
Maryville, IL 62062

Attorneys for Plaintiffs

/s/ *Raj Shah*
Raj N. Shah